Journal of Scientech Research and Development
Volume 3, Issue 1, June 2021
P-ISSN: 2715-6974 E-ISSN: 2715-5846
Open Access at: http://idm.or.id/JSCR

PENGEMBANGAN APLIKASI KEAMANAN PESAN TEKS MENGGUNAKAN ALGORITMA KRIPTOGRAFI ELGAMAL BASED ANDROID

DEVELOPMENT OF TEXT MESSAGE SECURITY APPLICATION USING ELGAMAL CRYPTOGRAPHIC ALGORITHM BASED ON ANDROID

Danyl Mallisza
Program Diploma III Manajemen Informatika Fakultas Ekonomi Universitas Ekasakti
E-mail: *danylmallisza2483@gmail.com*

INFO ARTIKEL

Koresponden

Danyl Mallisza
danylmallisza2483@gmail.com

Kata kunci:

Kriptografi, ElGamal, Android

Website:
http://idm.or.id/JSCR

hal: 52 – 62

ABSTRAK

Penelitian ini bertujuan untuk merancang dan membuat sebuah aplikasi untuk keamanan pesan. Pesan teks atau SMS (Short Message Service) adalah salah satu cara komunikasi yang populer. Namun, keamanan pesan seringkali menjadi perhatian utama pengguna. Oleh karena itu, penelitian ini bertujuan untuk mengembangkan aplikasi keamanan pesan teks dengan menggunakan algoritma kriptografi ElGamal berbasis Android. Aplikasi yang dibangun akan mengenkripsi pesan teks sebelum dikirim, sehingga hanya penerima yang dimaksud yang dapat membaca pesan tersebut. Penggunaan algoritma ElGamal dipilih karena fitur keamanannya yang kuat dan sulit untuk diretas. Penelitian ini juga akan membandingkan keamanan aplikasi yang dibangun dengan aplikasi pesan teks biasa. Hasil penelitian menunjukkan bahwa aplikasi yang dibangun lebih aman dalam mengirim dan menerima pesan teks. Penggunaan aplikasi ini diharapkan dapat memberikan keamanan tambahan bagi pengguna dalam bertukar pesan teks.

ARTICLE INFO

Correspondent:

Danyl Mallisza
danylmallisza2483@gmail.com

Key words:

elgamal, android, cryptography

Website:
http://idm.or.id/JSCR

page: 63 - 73

ABSTRACT

This research aims to design and create an application for message security. Text messages or SMS (Short Message Service) are a popular way of communication. However, message security is often a primary concern for users. Therefore, this research aims to develop a text message security application using the Android-based ElGamal cryptographic algorithm. The application that is built will encrypt text messages before they are sent, so that only the intended recipient can read the message. The use of the ElGamal algorithm was chosen because of its strong security features and is difficult to hack. This research will also compare the security of applications built with ordinary text messaging applications. The research results show that the application built is safer in sending and receiving text messages. The use of this application is expected to provide additional security for users when exchanging text messages.

PENDAHULUAN

Saat ini, penggunaan pesan teks sebagai sarana komunikasi sangat umum. Namun, keamanan pesan yang dikirim melalui pesan teks sering menjadi kekhawatiran, terutama dengan meningkatnya ancaman siber. Oleh karena itu, pengembangan aplikasi pesan teks yang aman sangat penting untuk memastikan kerahasiaan dan integritas pesan yang ditukar.

Studi ini bertujuan untuk mengembangkan aplikasi keamanan pesan teks menggunakan algoritma kriptografi ElGamal berbasis sistem operasi Android. Algoritma ElGamal dipilih karena fitur keamanannya yang kuat, yang membuatnya sulit bagi peretas untuk mengintersep dan mendekripsi pesan (Sholeh & Ferdiansyah, 2018).

Salah satu cara untuk melindungi pesan-pesan tersebut adalah dengan menggunakan teknik enkripsi. Enkripsi adalah proses mengubah isi pesan asli menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang. Dalam penelitian ini, akan dirancang sebuah aplikasi keamanan pesan singkat yang menggunakan algoritma ElGamal pada sistem operasi Android (Warnilah & Nugraha, 2018).

Algoritma ElGamal merupakan salah satu algoritma kriptografi kunci publik yang dapat digunakan untuk melakukan enkripsi pesan. Dalam algoritma ini, pesan akan dienkripsi dengan menggunakan kunci public (Alfiah et al., 2020), sedangkan untuk mendekripsinya, digunakan kunci privat yang hanya diketahui oleh penerima pesan (Fauzi et al., 2017).

Dalam kriptografi terdapat metode yang cukup penting dalam pengamanan data, yaitu dengan metode ElGamal untuk mengekripsi data yang berjalan pada sistem operasi Android sehingga pemilik telepon seluler yang berbasis android dapat melakukan pertukuran data SMS dengan lebih aman dan nyaman (Adhar, 2014).

Dalam menjaga kerahasian SMS, dibutuhkan suatu cara untuk mengamankan informasi yang sifatnya penting atau rahasia, yaitu dengan melakukan enkripsi terhadap teks SMS maka tingkat kemanan informasi dari pesan tersebut dapat ditingkatkan (David et al., 2021).

Dalam era digitalisasi seperti sekarang ini, penggunaan pesan singkat atau SMS menjadi salah satu bentuk komunikasi yang banyak digunakan oleh masyarakat (Nugroho et al., 2019). Namun, dalam penggunaannya, terkadang pesan-pesan tersebut mengandung informasi yang bersifat pribadi atau rahasia yang perlu dilindungi dari akses yang tidak sah. Oleh karena itu, diperlukan suatu mekanisme pengamanan untuk melindungi pesan-pesan tersebut agar tidak mudah dibaca oleh pihak yang tidak berwenang (Mei & Juni, 2019).

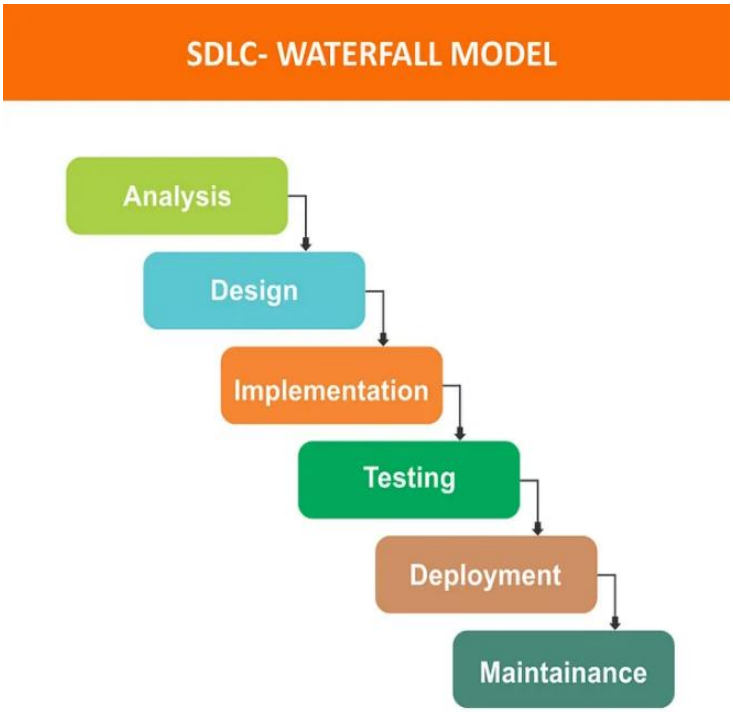
Aplikasi yang dikembangkan akan memberikan pengguna platform yang aman untuk bertukar pesan teks, memastikan bahwa pesan dienkripsi sebelum dikirim dan didekripsi hanya oleh penerima yang dimaksud. Penggunaan sistem operasi Android juga akan memberikan kenyamanan dan kemudahan penggunaan bagi pengguna (Junirianto, 2019).

Dengan adanya aplikasi keamanan pesan singkat ini diharapkan dapat memberikan perlindungan yang lebih baik terhadap pesan-pesan yang mengandung informasi penting agar tidak mudah diakses oleh pihak yang tidak berwenang. Selain itu, penelitian ini juga diharapkan dapat memberikan kontribusi dalam pengembangan teknologi keamanan informasi di Indonesia (Karima & Saputro, 2016).

Secara keseluruhan, pengembangan aplikasi ini diharapkan dapat berkontribusi pada peningkatan keamanan pesan teks dan meningkatkan perlindungan privasi pengguna.

METODE PENELITIAN

Metode yang digunakan pada penelitian ini menggunakan metode SDLC dengan model Model Waterfall (Pricillia & Zulfachmi, 2021), sebagai pendekatan pengembangan perangkat lunak yang linear, memberikan kerangka kerja yang terstruktur dan terurut untuk pengembangan aplikasi keamanan pesan teks menggunakan algoritma kriptografi ElGamal di platform Android. Dalam konteks judul penelitian "**Pengembangan Aplikasi Keamanan Pesan Teks Menggunakan Algoritma Kriptografi Elgamal Based Android**," setiap tahap model Waterfall berkontribusi secara sistematis untuk mencapai tujuan penelitian yang telah ditetapkan. Berikut adalah gambar dan penjelasan alur siklus model Waterfall :



Gambar 1. Siklus SDLC Model Waterfall

1. **Analisis (Analysis)**
   Tahap analisis berfokus pada pemahaman mendalam terhadap kebutuhan pengguna dan tujuan aplikasi. Tim akan melakukan analisis keamanan, mengidentifikasi kebutuhan fungsional dan non-fungsional, serta menetapkan batasan-batasan aplikasi untuk menggambarkan ruang lingkup dan tujuan yang harus dicapai.
2. **Desain (Design)**
   Setelah kebutuhan dan analisis selesai, tahap desain dimulai. Tim pengembang akan merancang arsitektur aplikasi keamanan pesan teks, termasuk desain antarmuka pengguna yang ramah pengguna dan perancangan struktur database untuk menyimpan pesan yang terenkripsi menggunakan algoritma kriptografi ElGamal.
3. **Implementasi (Implementation)**
   Tahap implementasi memanfaatkan desain yang telah dibuat sebelumnya dan menerjemahkannya ke dalam kode program. Algoritma kriptografi ElGamal diimplementasikan pada platform Android untuk memberikan keamanan maksimal dalam pertukaran pesan teks.
4. **Pengujian (Testing)**
   Setelah implementasi selesai, aplikasi akan menjalani serangkaian pengujian fungsionalitas dan keamanan. Pengujian ini mencakup verifikasi kinerja algoritma kriptografi ElGamal dan pengecekan keamanan aplikasi secara keseluruhan untuk memastikan perlindungan yang optimal terhadap pesan teks yang dipertukarkan.

5. **Pemeliharaan (Maintenance)**

   Tahap pemeliharaan terjadi setelah aplikasi diluncurkan. Tim pengembang akan terus memantau dan mengevaluasi kinerja aplikasi, merespons umpan balik pengguna, dan melakukan perbaikan atau peningkatan sesuai kebutuhan. Pemeliharaan ini bertujuan untuk menjaga keberlanjutan dan keamanan aplikasi seiring waktu.

Dengan mengikuti model Waterfall secara terstruktur, maka pengembangan aplikasi keamanan pesan teks dapat dilakukan dengan lebih terorganisir dan efisien, memastikan bahwa setiap tahap berkaitan erat dengan tujuan penelitian dan memberikan hasil yang diharapkan.

HASIL DAN PEMBAHASAN

Proses uji coba dari aplikasi ini dengan melakukan pengujian langsung terhadap pesan yang akan dienkripsi maupun didekripsi. Pada pembuatan aplikasi ini dibuat keamanan sistem data SMS yang mana dalam program ini pesan yang akan dikirim terenkripsi dengan menggunakan algoritma yang sudah ditentukan.

Pada umumnya orang mengirim pesan tanpa menggunakan enkripsi, jadi pada pengiriman pesan bisa dihacker atau diseludupi orang yang tidak bertanggung jawab. Oleh karena itu, dibuat perancangan aplikasi enkripsi data pesan singkat dengan menggunakan algoritma ElGamal berbasis android, yang mana program ini dibuat dengan sebaik mungkin.

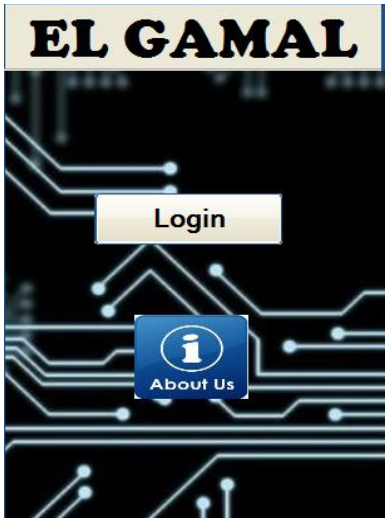
Dengan adanya program ini menambah keamanan dalam mengirim pesan yang rahasia kepada kepada penerima tanpa diketahui oleh orang lain. Aplikasi ini sangat mudah dipahami dan dipelajari dan aplikasi ini bisa dijalankan didalam *Smartphone*.

Tampilan Layar

Pada bagian ini merupakan penjelasan dari hasil rancangan interface untuk administrator yang terdiri dari sebagai berikut:

1. Laman Utama

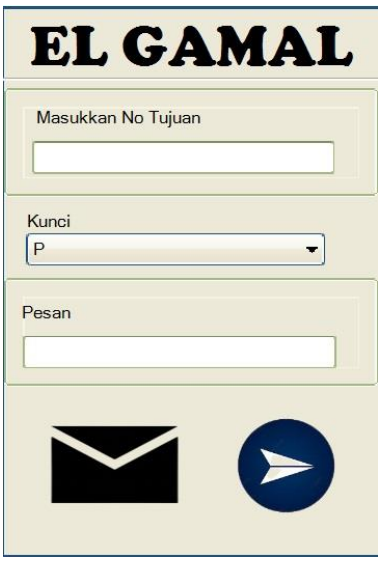
Pada antarmuka menu ini, terdapat formulir yang disediakan bagi pengguna untuk mengakses sistem atau menjalankan aplikasi yang telah dirancang. Menu ini menyajikan beberapa formulir yang memiliki fungsi khusus masing-masing. Detail antarmuka menu dapat ditemukan dalam gambar 2 yang terlampir.



Gambar 2. *Interface Menu Utama*

2. Laman Menu

Pada tampilan menu ini, terdapat formulir yang disiapkan untuk memungkinkan pengguna menjalankan aplikasi pesan yang telah dipersiapkan. Dalam menu ini, terdapat opsi untuk melakukan fungsi enkripsi pesan dan mengirim pesan. Rincian antarmuka menu ini dapat diakses melalui Gambar 3 yang terlampir.



Gambar 3. *Interface* Menu Tulis Pesan

Desain menu pada aplikasi untuk keamanan data pesan singkat dapat diuraikan sebagai berikut. Pertama, terdapat opsi "No tujuan" yang berfungsi untuk memasukkan nomor tujuan. Selanjutnya, opsi "Kontak" digunakan untuk mengambil nomor tujuan dari penyimpanan nomor yang tersedia. Terdapat juga opsi "Kunci p, g" yang berfungsi untuk menginputkan kunci publik yang diperlukan dalam proses enkripsi pesan. Selanjutnya, opsi "Kunci x" digunakan untuk memasukkan kunci privat sebelum melakukan proses enkripsi pesan. Selain itu, terdapat opsi "Pesan" yang berfungsi untuk memasukkan teks pesan yang akan dienkripsi. Tombol "Enkripsi" akan memproses enkripsi pesan tersebut, dan hasilnya akan ditampilkan melalui opsi "Hasil". Terakhir, terdapat tombol "Kirim" yang berfungsi untuk mengirimkan pesan yang telah dienkripsi.

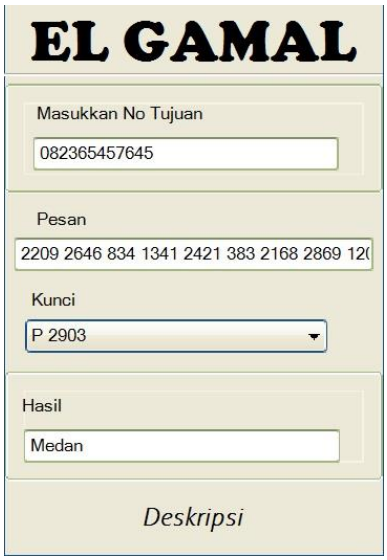
3. Laman Form Enkripsi

Berikut Formulir ini muncul setelah berhasil melakukan proses pengenkripsian sebuah pesan. Tampilan formulir hasil enkripsi dapat diakses melalui Gambar 4 yang terlampir.

Gambar 4. *Interface Form* **Hasil** *Enkripsi*

4. Laman Form Interface proses Dekripsi

Berikut adalah tampilan Formulir deskripsi, laman ini muncul setelah proses dekripsi pesan berhasil dilaksanakan. Tampilan formulir hasil dekripsi dapat diakses melalui Gambar 5 yang terlampir.



Gambar 5. Interface Form Hasil Dekripsi

Pengujian

Pada tahan pengujian aplikasi ini menggunakan UJI BLACK BOX, Pengujian black box (black box testing) adalah metode pengujian perangkat lunak yang menitikberatkan pada aspek fungsionalitas. Tahap pengujian merupakan komponen esensial dalam siklus pengembangan perangkat lunak, bersama dengan tahap perancangan. Berikut adalah hasil pengujian sistem menggunakan metode blackbox testing yang disajikan dalam tabel pengujian blackbox seperti yang tertera di bawah ini.

Tabel 1. Hasil Pengujian Black Box Aplikasi Enkripsi Teks

No	Laman	Keterangan	Hasil
1	Masuk ke aplikasi Enkripsi Teks	Sistem akan memulai aplikasi dengan menampilkan layar pembuka aplikasi dan beralih ke menu pilihan.	Valid
2	Memilih menu pesan	Akan mengakses formulir untuk menulis pesan.	Valid
3	Pilih opsi untuk menulis pesan, masukkan nomor tujuan, input kunci, lakukan enkripsi pesan, dan kirim Pesan.	Menghasilkan teks biasa (plainteks) yang disimpan di dalam kotak masuk.	Valid
4	Lanjutkan pada proses dekripsi dengan memeriksa kotak masuk dan memasukkan kunci, kemudian klik pada hasil.	Menghasilkan teks terenkripsi (chiperteks) yang telah berhasil didekripsi.	Valid
5	Mengamati pesan yang telah dikirim.	Akan muncul hasil yang telah dikirim.	Valid
6	Memilih menu *about*	Akan tampil menu *About*	Valid

Analisa Hasil

Berikut adalah langkah-langkah dalam prosedur pembangkitan kunci sistem kriptografi ElGamal:

1. Pemilihan Kunci Publik Pertama (p): Pilih sebuah bilangan prima yang lebih besar dari 255 sebagai kunci publik pertama (p).
2. Penentuan Kunci Privat (x): Kunci privat (x) dihasilkan secara acak dari bilangan antara 1 hingga p – 2.
3. Pemilihan Kunci Publik Kedua (g): Kunci publik kedua (g) dipilih sebagai bilangan yang dimulai dari 2, 3, 4, 5, dan seterusnya, hingga hasil perhitungan g^((p-1)/2) mod p tidak sama dengan 1.
4. Perhitungan Kunci Publik Ketiga (y): Kunci publik ketiga (y) dihitung menggunakan rumus y = gx mod p.

Tabel 2. Kunci Kriptografi ElGamal

Kunci Publik P	Kunci Publik G	Kunci Privat X
2903	6	11
863	5	373
911	7	199
719	11	631
2909	7	13

Hasil Pengujian Enkripsi

Dijelaskan pada tabel di bawah ini menampilkan hasil pengujian enkripsi karakter pesan menggunakan kunci publik P = 2903, G = 6, dan kunci privat X = 11.

Tabel 3. Hasil Pengujian Enkripsi

No	Karakter	Desimal	k	C1=G^k Mod P	C2=Y^k m Mod P
1.	M	117	784	2209	2646
2.	e	116	2315	834	1341
3.	d	97	826	2421	383
4.	a	109	422	2168	2869
5.	n	97	2806	1205	2614

Hasil Pengujian Dekripsi

Berikut ini adalah tabel hasil pengujian dekripsi pesan karakter dengan menggunakan kunci publik P = 2903 kunci privat X = 11.

Tabel 4. Hasil Pengujian Dekripsi

No	C1	C2	D={$C1^{p-x-1}$. C2} Mod P	Karakter
1.	2209	2646	77	M
2.	834	1341	101	e
3.	2421	383	100	d
4.	2168	2869	97	a
5.	1205	2614	110	n

Kelebihan Dan Kekurangan

Kelebihan aplikasi yang dirancang adalah sebagai berikut:

1. Aplikasi dapat menjaga keamanan dan kerahasiaan pesan dari orang yang tidak bertanggung jawab.
2. Aplikasi ini bekerja dengan kombinasi dari tiga kunci publik dan satu kunci privat yang merupakan bilangan prima.
3. Mempermudah user dalam mengamankan data.
4. Mudah digunakan karena user interface yang sederhana

Sedangakan sebagai kekurangan aplikasi yang dirancang adalah sebagai berikut:

1. Tampilan dan layout dari aplikasi masih sederhana.
2. Proses enkripsi hanya bisa dilakukan pada pesan karakter saja, tidak bisa file audio, gambar dan video.
3. Biaya untuk kirim pesan yang telah di enkripsi menjadi Chipertext akan lebih besar, karena panjang hasil enkripsi pesan menjadi dua kali lipat dari sebelumnya.
4. Ketika mengenkripsi pesan dengan jumlah karakter yang terlalu panjang akan memakan waktu yang cukup lama.

SIMPULAN DAN SARAN

Simpulan

1. Penerapan algoritma kriptografi elgamal pada program yang telah dibuat adalah sesuai dengan proses algoritma kriptografi elgamal yang ada. Hal ini dibuktikan dengan terbentuknya pasangan kunci publik dan kunci privat.
2. Kunci publik yang dihasilkan terdiri dari tiga buah bilangan yaitu nilai p,g dan y dan kunci privat hanya satu yaitu nilai x.
3. Hasil enkripsi yang dihasilkan memiliki panjang dua kali lipat dari panjang plaintext awal. Hal ini dikarenakan setiap blok plaintext dienkripsi dengan

mencari pasangan *chipertext* $a = g^k \bmod p$ dan $b = y^k m \bmod p$. Sehingga menghasilkan pasangan (a,b).

4. Algoritma kriptografi elgamal dapat diterapkan pada bahasa pemrogram java untuk pengamanan pesan.

Saran

1. Perlu dilakukan pengembangan atau perbaikan pada desain interface agar lebih memudahkan pengguna dalam menggukan aplikasi ini.
2. Jenis file yang dapat diekripsi hendaknya bukan hanya file teks saja tetapi mencakup beberapa file seperti file gambar, video atau suara.
3. Perlunya dilakukan kombinasi dari dua atau lebih algoritma kriptografi agar lebih menjamin tingat keamanan data.

DAFTAR PUSTAKA

Adhar, D. (2014). Pengamanan Sqlite Database Menggunakan Kriptografi Elgamal. *Snif*, *Vol.1*(No.1), 432–437.

Alfiah, F., Sudarji, R., & Taqiyyuddin Al Fatah, D. (2020). *Aplikasi Kriptografi Dengan Menggunakan Algoritma Elgamal Berbasis Java Desktop Pada Pt. Wahana Indo Trada Nissan Jatake* (p. 12260).

David, S., Atmam, & Widi, setiawan. (2021). Algoritma Kriptografi Kunci Publik Elgamal Untuk Keamanan Pesan Sms (Short Message Service) Berbasis Android. *Teknik*, *15*(x), 1–8.

Fauzi, A., Maulita, Y., & Novriyenni. (2017). Perancangan Aplikasi Keamanan Pesan Menggunakan Algoritma Elgamal Denganmemanfaatkan Algoritma One Time Pad Sebagai Pembangkit Kunci. *Jurnal Teknik Informatika Kaputana (JTIK)*, *1*(1), 1–9.

Junirianto, E. (2019). Pengembangan Aplikasi Evaluasi Dosen Berbasis Android dengan Keamanan Json Web token (JWT). *JOINTECS (Journal of Information Technology and Computer Science)*, *4*(3), 87. https://doi.org/10.31328/jointecs.v4i3.1066

Karima, A., & Saputro, A. (2016). Pembangkitan Kunci pada Algoritma Asimetris ElGamal untuk Meningkatkan Keamanan Data bertipe .docx. *Sisfotenika*, *6*(2), 170–181. https://doi.org/10.30700/jst.v6i2.120

Mei, A., & Juni, P. (2019). *Pengaruh Sistem Pengamanan Data Pasien di Rumah Sakit Menuju Era Revolusi Industri 4.0*. *269*, 106–114.

Nugroho, F. P., Abdullah, R. W., Wulandari, S., & Hanafi. (2019). Keamanan Big Data di Era Digital di Indonesia. *Jurnal Informa*, *5*(1), 28–34.

Pricillia, T., & Zulfachmi. (2021). Perbandingan Metode Pengembangan Perangkat Lunak (Waterfall, Prototype, RAD). *Jurnal Bangkit Indonesia*, *10*(1), 6–12. https://doi.org/10.52771/bangkitindonesia.v10i1.153

Sholeh, J., & Ferdiansyah, F. (2018). Implementasi Kriptografi Email Berbasis Android Dengan Metode Elgamal Pada Pt Sudata Makmur. *Skanika*, *1*(2), 662–668. http://jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/273

Warnilah, A. I., & Nugraha, S. N. (2018). Komparasi Algoritma Kriptografi Elgamal Dan Caesar Cipher Untuk Enkripsi Dan Dekripsi Pesan. *IJCIT (Indonesian Journal on Computer and Information Technology)*, *3*(2), 243–252.

https://doi.org/10.31294/ijcit.v3i2.4671

Wahid, A. A. (2020). Analisis metode waterfall untuk pengembangan sistem informasi. J. Ilmu-ilmu Inform. dan Manaj. STMIK, no. November, 1-5.

Udi, U. (2018). Penerapan Metode SDLC Waterfall Dalam Pembuatan Sistem Informasi Akademik Berbasis Web Studi Kasus Pondok Pesantren Al-Habib Sholeh Kabupaten Kubu Raya, Kalimantan Barat. Jurnal Teknologi Dan Manajemen Informatika, 4(1).

Alfiah, F., Sudarji, R., & Al Fatah, D. T. (2020). Aplikasi Kriptografi Dengan Menggunakan Algoritma Elgamal Berbasis Java Desktop Pada Pt. Wahana Indo Trada Nissan Jatake. ADI Bisnis Digital Interdisiplin Jurnal, 1(1), 22-34.